The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions

Christina Katsini
Human Opsis
Patras, Greece
ckatsini@humanopsis.com

Yasmeen Abdrabou
Bundeswehr University
Munich, Germany
yasmeen.essam@unibw.de

George E. Raptis
Human Opsis
Patras, Greece
graptis@humanopsis.com

Mohamed Khamis
University of Glasgow
Glasgow, United Kingdom
mohamed.khamis@glasgow.ac.uk

Florian Alt
Bundeswehr University
Munich, Germany
florian.alt@unibw.de

ABSTRACT

For the past 20 years, researchers have investigated the use of eye tracking in security applications. We present a holistic view on gaze-based security applications. In particular, we canvassed the literature and classify the utility of gaze in security applications into a) authentication, b) privacy protection, and c) gaze monitoring during security critical tasks. This allows us to chart several research directions, most importantly 1) conducting field studies of implicit and explicit gaze-based authentication due to recent advances in eye tracking, 2) research on gaze-based privacy protection and gaze monitoring in security critical tasks which are under-investigated yet very promising areas, and 3) understanding the privacy implications of pervasive eye tracking. We discuss the most promising opportunities and most pressing challenges of eye tracking for security that will shape research in gaze-based security applications for the next decade.

Author Keywords

Eye tracking; Gaze Interaction; Security; Privacy; Survey

CCS Concepts

•Security and privacy → Human and societal aspects of security and privacy; •Human-centered computing → Human computer interaction (HCI);

INTRODUCTION

The security community is an early adopter of eye tracking. Security researchers have explored the use of eye tracking for biometric authentication [14, 67, 107, 108] and password entry [53, 93] since the early 2000s. Twenty years later, eye tracking algorithms and technologies have matured significantly. Recent advances in visual computing, gaze estimation algorithms, cameras, and processing power of computing devices have led to eye tracking being no longer constrained to desktop computers but being also available on head-mounted displays [6, 45, 49, 52, 103], handheld mobile devices [73], and public displays [171]. Today, laptops such as Alienware 17 R4 and Acer Predator 21 X come with integrated eye trackers, and smartphones such as the iPhone X and Huawei Mate 30 Pro are equipped with front-facing depth cameras, capable of accurate gaze estimation. Eye trackers are also now used in driver monitoring systems in BMW [17] and Volvo cars [166].

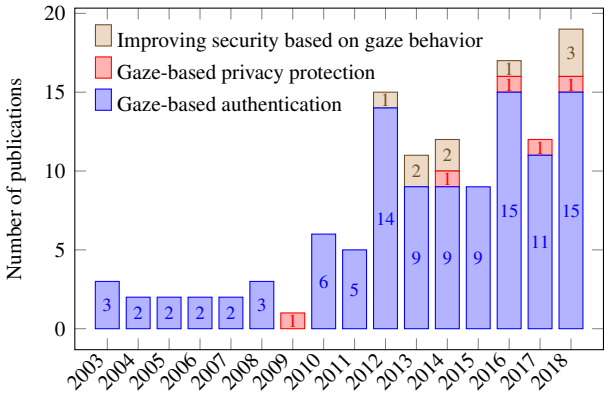

Figure 1. Security researchers are among the first to adopt eye tracking for gaze-based security applications. We classified work from related publications based on the utility of gaze: a) authentication, b) privacy protection, and c) improving security by understanding users through their gaze behavior. The figure highlights that there has been an increase in contributions in this area largely due to the maturity and accessibility of the eye tracking hardware and software. It is also clear that some areas received less attention than others albeit being equally promising.

These are important developments for security applications. The ubiquity of eye tracking means that researchers can finally take their gaze-based security applications to the real world. The benefits of large-scale eye tracking include: 1) higher adoption of gaze-based security applications (e.g., gaze-based privacy protection or gaze-based authentication), which in turn leads to better understanding their effectiveness and performance in daily scenarios, 2) allowing more gaze data to be collected that can be used to improve existing approaches (e.g., to improve the accuracy of biometric authentication), and 3) the ability to unobtrusively understand users through their gaze behaviour during security critical tasks (e.g., understanding gaze behavior when subject to phishing attacks).

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

http://dx.doi.org/10.1145/3313831.3376840

Despite the significant potential this creates from both a security and a user experience perspective, a holistic view of how research on gaze-based security applications developed in the past decades is missing. This paper closes this gap by a) surveying and organizing knowledge in this field based on previous work in the area, b) clustering existing work into three main application areas: gaze-based authentication, gaze-based privacy protection, and gaze monitoring during security tasks, and c) highlighting the most promising opportunities and most pressing challenges that require further research.

We present 8 important and promising directions for future research in this area and identify 2 challenges that need to be addressed as they hinder the adoption of gaze-based security applications. For example, we highlight that the recent developments in the area make it possible to conduct field studies for gaze-based security applications. This was until recently infeasible due to limitations in mobile eye tracking hardware. We discuss other research opportunities, such as blending implicit gaze-based authentication with everyday tasks and privacy protection by estimating users' and bystanders' gaze. We also underline challenges that are important to address in upcoming HCI research, such as understanding the privacy implications of pervasive eye tracking and the trade off between the accuracy and speed of gaze-based security applications.

RELATED WORK

There have been attempts to organize the existing research in eye tracking for security applications. Most of those focused on the use of physiological biometrics (e.g., iris [24, 111, 117], retina [24, 111, 117], periocular [117]) for building and evaluating authentication schemes, without considering the use of gaze-based features. Many works apply gaze-based features to build an authentication scheme, aiming to overcome the limitations that are introduced by the use of physiological biometrics, such as inability to revoke passwords once compromised, or unintentional authentications [146]. Most surveys considering eye gaze do not address the HCI perspective but focus on technical [174] and methodological [47] aspects of such systems (e.g., the use of bio-signals for human identification [41]). None of the existing surveys consider multi-factor gaze-based authentication, gaze-based privacy protection, or the use of gaze to understand users during security tasks. To our knowledge, this is the first survey to holistically cover the three major utilities of gaze in security applications.

In short, we focus on the use of eye gaze in security and privacy applications from an HCI perspective. We do not consider work on the use of physiological-only biometrics nor work that is solely based on the technical aspects of gaze-based security and privacy applications. Our contribution is twofold: **(1)** we survey research manuscripts and classify previous work based on the utility of gaze in security applications; **(2)** we highlight promising HCI research directions and challenges that hinder the uptake of gaze-based security applications.

METHODOLOGY

A number of surveys served as a starting point for our review [41, 47, 111, 117, 138, 145, 174]. Additionally, we used the following search terms and all their combinations to obtain the papers that formed the basis of our literature review: ("eye tracking" OR "Gaze") AND ("security" OR "privacy" OR "authentication" OR "password" OR "biometric"). We considered papers published in HCI, UbiComp, Eye Tracking, and Security conferences or journals: CHI, IJHCS, HCI, UbiComp/IMWUT, MobileHCI, IJHCI, ETRA, CVPR, CCS, SOUPS, USENIX Security, S&P, and NDSS. We started with this initial set and then additionally conducted backward and forward reference searching in the papers we collected.

We examined the set and excluded papers that were not written in English, not related to our research objective (e.g., systems that are solely based on physiological data), papers that reported the same studies (e.g., a research team published their work in a journal but subsequent articles were published in workshops) and non peer-reviewed works (e.g., master theses and technical reports).

We coded each paper of the final set based on the utility of gaze in security applications, and, finally, we identified three main categories: 1) Authentication: gaze was used for explicit, implicit, and multi-factor authentication; 2) Privacy protection: gaze was used to protect the privacy of users (e.g., displaying content that is being looked at while hiding the rest from shoulder surfers); 3) Improving security based on gaze behavior: by analyzing the gaze behavior, systems can uncover user properties (e.g., nervousness when reading a phishing email, or carelessness when creating a password), and intervene accordingly to improve security.

We returned to the papers and summarized them to identify their motivations, methodologies, and contributions to gaze-based security and privacy research.

AUTHENTICATION

Gaze has many advantages in the context of authentication. Namely, eye movements can be subtle and hard to notice, making gaze attractive for observation-resilient and high-entropy authentication. These reasons encouraged researchers to investigate ways to leverage gaze for explicit and implicit authentication. We summarize three lines of work: 1) explicit gaze-based authentication, 2) implicit gaze-based authentication, and 3) gaze-supported multi-factor authentication.

EXPLICIT GAZE-BASED AUTHENTICATION

Explicit gaze-based authentication refers to the use of eye movements to explicitly verify identity. In this type of authentication, the user has to first define a password that involves consciously performing certain eye movements (step 1: password creation). The user then authenticates by recalling these eye movements and providing them as input (step 2: password recall). The system detects the eye movements and compares them to the password defined in step 1 to verify users' identity.

Researchers have explored a wide variety of eye movements that could be used for authentication. This includes fixations [93], gestures [33, 34], and smooth pursuit eye movements [8, 27, 35, 164]. There are two dimensions to consider in the use of gaze for explicit authentication: a) password type: legacy vs gaze-based password symbols, and b) used modalities: unimodal vs multimodal gaze-based authentication.

Legacy vs Gaze-based Password Symbols

The first dimension refers to the type of password. Passwords in gaze-based explicit authentication can have two forms: 1) gaze can be used as a modality for entering *legacy passwords* (e.g., PINs, text passwords or graphical password), or 2) gaze can be used to enter a *gaze-based password* where the password's symbols are made of eye movements (e.g., a password that involves gazing to the left, then gazing to the right).

Legacy Passwords

Each password consists of a series of symbols. Traditional systems have used PINs and passwords (i.e., a series of digits and alphanumeric characters, respectively). Digits and alphanumeric characters are examples of legacy symbols that were argued to have been superseded, but it is difficult to replace them because of their wide use as they are easy to implement and easy to reset. Examples of systems that use legacy password symbols include banks and online websites. Gaze can support entering legacy symbols by providing a certain mapping between gaze behaviors and certain symbols. There are many examples of schemes employing gaze to enter legacy passwords. For example, Kumar et al. [93] proposed one of the first gaze-based authentication schemes where users fixated characters on an on-screen keyboard and then pressed the space button to select them. The same scheme was used on ATMs by Seetharama et al. [142]. Similar work was also done by Kasprowski et al. [63] who used gaze for pointing at PINs and confirmed selection by pressing a key. EyePassShapes uses eye movements to enter alphanumeric passwords [32].

Another body of work focused on using gaze to enter PINs. EyeDent [168] allows users to authenticate on desktops by entering 4-digit PINs using eye gaze. Users do not dwell or press triggers. Instead, the system automatically clusters the gaze points to estimate which targets the user intended to select. PathWord [8] is another system where users enter 4-digit PINs by performing smooth pursuit eye movements that follow the trajectory of the respective digits. GazeTouchPIN [79] allows users to enter 4-digit PINs on mobile devices using touch and gaze input. Liu et al. [102] explored using gaze gestures to enter 4-digit PINs on smartphones. Best and Duchowski [15] proposed using gaze to enter PINs on a rotary dial interface.

Several works used smooth pursuit eye movements to allow users to enter 4-digit PINs on a public display [27, 80, 83]. Other researchers explored the augmentation of graphical password schemes by using gaze input. For example, in the work of Forget et al. [43,44], Bulling et al. [20] and others [10,86,157], users fixated points on a shown image, using their gaze as an alternative to clicking with the mouse. Similarly, George et al. [49] used gaze to input 3D graphical passwords in VR. Another authentication scheme that has been extended using gaze input is PassFaces [129]; several works [37, 53] extended PassFaces to allow gaze-based selection based on fixations. In EyeSec [98], the authors propose using gaze for input on multiple existing systems, including PIN pads and Patterns.

The advantage of using gaze to enter legacy password symbols is that they can easily integrate with existing backends. For example, to employ EyePIN [33] at an ATM that accepts 4-digit PINs, all that is needed is a camera to track the user's eyes. However, the disadvantage is that the schemes might induce additional cognitive load on the user in order for them to understand the mapping between their gaze and the resulting symbol. Furthermore, most of these schemes are significantly slower to use compared to traditional, less secure alternatives. For example, GazeTouchPIN [79] and EyePassword [93] require 10.8 and 9.2 seconds respectively to authenticate, while classical PINs require 1-1.5 seconds only [167].

Gaze-based Passwords

Gaze-based passwords are based on gaze behavior. These schemes transform the password space and, hence, are likely to have a different impact on memorability. Examples include GazeTouchPass [74] and GTmoPass [78], where gaze gestures constitute part of the password. Similarly, in EyePass [34] and another work by De Luca et al. [33], the password consists of a series of gaze gestures. In DyGazePass [126, 127], the user's input is a series of smooth pursuit movements that are supported by cues in the form of 2D geometric objects. In EGBP [141], users authenticate by gazing in one of four directions and then performing a blink to confirm input.

The advantage of gaze-based passwords is that they expand the password space by incorporating new sets of password symbols. Unlike legacy passwords where PINs, alphanumeric, and other widely used passwords are entered by gaze, gaze-based passwords might have a steeper learning curve as users are not accustomed to them, and require in-depth analysis of memorability as users would be required to learn and memorize unfamiliar password symbols which could be less intuitive.

RESEARCH DIRECTION 1

Selecting and Recalling Gaze-based Passwords

Authentication schemes that leverage touch, mid-air gestures, or tactile input make use of the user's muscle memory [144]. At the same time, the eyes are perceptual rather than control organs. There is no evidence so far that eye movements tap into muscle memory. This raises questions about the memorability of gaze-based authentication. For example, is it harder to recall legacy passwords when entered using gaze as opposed to other modalities? Does the process of recalling a password rely more on the input behaviour (e.g., finger movements vs eye movements during password input), or does it rely on the memorized password itself (e.g., 1234 vs gaze up, gaze down, gaze left). There has not yet been a direct comparison between memorability of legacy and gaze-based passwords. Also, it is unclear how users select gaze-based passwords and if their selections and perceptions of strong gaze-based passwords match reality. Prior work showed that users' perceptions of strong text passwords do not always match reality [161], but this has not yet been investigated for gaze. These gaps have not been addressed and are open directions for future research. Understanding this will allow the community to identify whether gaze-based passwords offer additional benefits, or if it is rather more practical to use gaze to input legacy passwords.

Unimodal vs Multimodal Gaze-based Authentication

Gaze has been used as the sole input method when authenticating. We refer to that type as unimodal gaze-based authentication. On the other hand, multimodal gaze-based authentication is when gaze is combined with other modalities.

Unimodal Gaze-based Authentication

The advantage of unimodal gaze-based schemes is that they are handsfree. This makes them particularly useful for interfaces that are physically unreachable (e.g., displays behind glass windows [31]), for users with motor disabilities, and for touchless hygienic interactions. The disadvantage, however, is that unimodal gaze-based interfaces need a mechanism to distinguish input and perception. That is, the system needs to detect whether a user is gazing at a target to select it, or merely to perceive it. This has been traditionally addressed by introducing a dwell duration, i.e., the user has to gaze at the target continuously for a brief predefined period of time in order to select it [60]. This method has been adopted by several unimodal authentication schemes [20, 33, 44]. An alternative is to detect certain gaze behaviors that would indicate input, such as gaze gestures [36] as done in EyePassShapes [32], or smooth pursuit eye movements [27, 83, 126, 127, 164].

Multimodal Gaze-based Authentication

In multimodal schemes, gaze is used a) as a pointing mechanism while another modality is used for selection (we refer to this as *gaze-supported multimodal authentication*); or b) alongside a second modality to improve resistance to observation attacks by *splitting the observer's attention*. The advantage of the former type is that, opposed to unimodal gaze input, the system can clearly distinguish input from perception as the user would use the second modality to confirm the intention to select the target being gazed at. Examples include EyePassword [93], GazeTouchPIN [79] and others [63], where users select each password symbol in two steps. Each step involves one of the modalities. In the latter type, gaze and other modalities are used together for improved protection against observation attacks. For example, users of GazeTouchPass [74], GazeGestureAuth [3] and GTmoPass [78] enter a series of gaze input alongside either touch input [74, 78] or mid-air gesture [3]. This requires shoulder surfers to observe two elements which in turn reduces attack success rates. The general disadvantage of multimodal authentication is that it usually complicates password entry. This could influence the memorability of the password symbols.

How to Evaluate Explicit Gaze-based Authentication

Users will, in general, not adopt a secure mechanism that is complicated to use and will find workarounds that reduce security (e.g., write down passwords). Therefore, it is important to make sure new schemes are both usable and secure.

Usability and Memorability Evaluation

Usability studies often include participants entering passwords using the new scheme, comparing it to a baseline – usually a state-of-the-art scheme. The user's task is to enter a password provided by the experimenter. The password could be verbally communicated to the user [79] or read by a text-to-speech system [83]. Requiring the participant to read passwords from a piece of paper or a screen [82] is not recommended for gaze-based authentication schemes as it might impact the tracked gaze behavior. Error rates are often measured by detecting input failures. A less used approach, albeit equally important, is to present users with incorrect inputs and ask them to correct them [82]. This provides insights on how recognizable errors are, and how easy, fast, and accurately users can correct them.

Memorability is often evaluated by querying participants after a period of time to understand whether they remember a) how to use the scheme, and b) their secret. Note that memorability is important to consider regardless of whether legacy or gaze-based password symbols are used. Even if users are entering the commonly used 4-digit PINs, the input method impacts the user's memory [32]. This underlines the importance of understanding memorability of proposed schemes.

Security Evaluation

Security studies of gaze-based input often focused on side channel attacks that can be performed by bystanders or co-located adversaries. Examples of studied attacks include observation attacks (e.g., shoulder surfing) [39] and video attacks [169]. In security studies that investigate shoulder surfing resistance, the user is often recorded while authenticating from the best observation angle possible. The recorded videos are then presented to a different set of participants who have been trained to attack passwords entered via the respective authentication scheme. For example, to evaluate GazeTouchPass [74], the experimenters recorded three videos: a) a video showing the user's eyes to simulate an attacker observing the user's eyes, b) a video showing the user's screen to simulate shoulder surfing the touch input, and finally c) a video from an angle that allows observing both the gaze and touch input.

Guessing attacks, which help understanding how likely an attacker will find a password by random or smart guesses, are also important to investigate. However, the lack of knowledge on how users select their gaze-based passwords (Research Direction 1) means that there are no established strategies that attackers use to make informed guesses.

Evaluation Metrics

Regarding the evaluation metrics, usability often entails efficiency (i.e., entry time) and efficacy (i.e., error rate due to system malfunction or user errors). Other aspects that can be considered include error tolerance (i.e., how likely is it that users perform errors), learnability (i.e., how easy/fast users can learn how to use the scheme), and user preference. In memorability studies, the metrics are often the recall rate and the recall accuracy. The latter is a measure of similarity of how close the user's recalled password is to the actual password.

Metrics that are commonly used in security studies are: a) attack success rate and b) attack accuracy. The former refers to whether or not attacks were successful while the latter measures how similar the attacker's guess is to the actual password. These values are measured under a threat model that simulates an attack scenario. Suitable threat models should be employed when evaluating the security of authentication schemes. For example, previous work evaluated multimodal authentication schemes against two observers [76] and by using video record-

ings from two cameras [74]. Commonly studied threats include shoulder surfing attacks [39], video attacks [32], thermal attacks [1], and smudge attacks [11]. While gaze input is not vulnerable to thermal or smudge attacks, multimodal authentication schemes involving touch or tangible input might leak heat or smudge traces that make the scheme vulnerable to said attacks. Studying the aforementioned threat models is important because new input methods do not impact backend security, but rather impact the possible side channel attacks.

Further metrics that could be used to evaluate security include the number of guesses required until an attack is successful. Finally, the theoretical password space should also be computed for any new authentication scheme, while the practical password space can be computed through a longitudinal in the wild study to understand what kind of passwords users create.

RESEARCH DIRECTION 2

Evaluating Explicit Authentication in the Wild

There are several evaluation paradigms in HCI research, each suitable for answering certain types of research questions. Lab studies are generally suited for quantitative measurements and collecting data in a controlled setting where external factors are reduced or ideally eliminated. However, lab studies suffer from low ecological validity as they do not reflect real life conditions. This is why the HCI community also embraces field studies where systems are evaluated in real scenarios such as in public.

Explicit gaze-based authentication was mainly investigated in the lab. As eye tracking technologies become cheaper [68], and soon to become ubiquitous on handheld mobile devices [73, 75], an emerging research opportunity is to evaluate authentication schemes in the wild. This would allow studying learnability to investigate if users' performance improve after continued daily usage, as well as social implications when using the schemes in public, such as social embarrassment, or unintentionally looking at bystanders when performing gaze input.

There is a lack of – and hence an opportunity for – field studies of explicit gaze-based authentication. This will allow a) collecting ecologically valid findings, not impacted by eye fatigue caused by multiple entries during studies, b) studying the impact of learning effects, c) studying long term memorability, and d) studying use in different contexts.

IMPLICIT GAZE-BASED AUTHENTICATION

Implicit Gaze-based Authentication refers to the use of eye movements to implicitly verify identity; it does not require the user to remember a secret, but it is based on inherent unconscious gaze behavior and can occur actively throughout a session. It consists of two steps: the *enrolment* phase during which a digital representation of eye movements is acquired and stored as a template and the *recognition* phase during which the eye movement is tracked, processed and compared to the template to establish the identity of the individual.

Ideally, the tracked eye movements should possess the characteristics of an ideal biometric: universality, uniqueness, permanence and collectability. Research in the field mainly focused on assessing unique eye movements when performing activities with varying visual stimuli and type (e.g., time-dependent). Collectability mainly depends on the context of use (e.g., device capabilities, eye tracking metrics). The permanence of the eye movements has not been fully explored in this context.

Context of Use and Design Perspectives

Identification vs Verification

In implicit authentication it is important to distinguish verification (verifying user's identity through a 1:1 comparison) from identification (i.e., discovering the user's identity through a 1:N search) as it affects the authentication performance [149]. In identification scenarios, the more users the system has, the more realistic and more difficult the problem is, and thus, the performance of the system heavily depends on the sample size, the classification models, the device capabilities, and the required resources. Several surveyed works (52) focus on identification (e.g., [13, 21, 26, 30, 55, 65, 114, 115, 132, 139, 163]) while relatively less (21) focus on verification (e.g., [4, 22, 56, 61, 149, 173]), which requires significantly less processing effort.

Eye Tracking Metrics

In contrast to explicit gaze-based authentication, eye-tracking metrics for implicit authentication schemes are more diverse, such as gaze entropy [16], fixation density map [97], angular saccade velocity [104], and scan-paths [55]. Researchers, after acquiring gaze data, extend their data sets considering metrics that build upon the fundamental acquired data (e.g., fixation duration, angles velocity) and calculations on them (e.g., mean, maximum, minimum values). The more eye tracking metrics are available for building identification and verification models, the higher the likelihood for improved performance. Several toolkits (e.g., EMDAT, EALab), can be used to process eye-tracking data and generate larger, more inclusive data sets.

The eye-tracking metrics are often complemented with physiological eye metrics [4, 14, 30, 90, 150] or technology-based metrics, such as key-stroke sequences [147] and mouse dynamics [65, 136] aiming to improve the performance of implicit gaze-based authentication. However, the integration with metrics from multiple and diverse sources introduces a higher level of interdependence and complexity, which could be a barrier when attempting to adopt such implicit authentication schemes in real-life scenarios and everyday tasks.

Device Capabilities

The extracted eye-tracking metrics depend on the eye tracker's capabilities, as they are associated with device-dependent specifications, such as operating distance, frequency, and operating window. Considering that eye trackers vary from sophisticated systems to simple embedded cameras, they have varying characteristics that influence the universality, the acceptance, and the performance of gaze-based implicit authentication. Considering that people use multiple devices with diverse characteristics, that issue becomes more intense. Very few research teams have considered the equipment when analysing and discussing the findings of their studies [38, 87, 165]. For example, Eberz

et al. [38] used a downsampling approach to show that different sampling rates affected the quality of eye-tracking metrics. Similar work was reported by others [57, 62].The trade-off between equipment features, the effort of developing sophisticated algorithms for implementing authentication mechanisms depending on sampling data, and processing requirements for using such a scheme in the wild remain unexplored.

RESEARCH DIRECTION 3

Context & Design of Implicit Authentication

Different contexts of use of implicit gaze authentication have not been explored. Yet, context may pose different requirements to interface design and processing. Questions such as how authentication is triggered, if identification or verification is required, etc. could guide the design decisions for implicit gaze-based authentication. Given that identification requires more resources compared to verification, understanding which contexts require identification (e.g., claim an online profile), which require verification (e.g., unlock mobile phone) and which require both (e.g., access email from unknown device) would enable research to focus on realistic scenarios. Apart from the interface, the authentication factors need to be designed (e.g., data type, task type, time to authenticate) and scenarios where implicit authentication is a better fit need to be explored.

Continuous vs Controlled Visual Stimuli

Two types of visual stimuli have been used in implicit gaze-based authentication: *controlled* and *continuous*. For controlled visual stimuli, people interrupt other tasks and focus their attention on this stimulus, thus being aware that they are going through an authentication task. Controlled visual stimuli can be either *static* or *dynamic*. Tasks that are based on static stimuli include text-based tasks [13, 14, 48, 56, 124, 133, 147], such as reading a passage excerpt, and static image-based tasks [14, 21, 25, 56, 104, 105, 115, 119, 132, 133, 150], such as the exploration of a photograph. The complexity of the images affects the accuracy of the scheme [150, 170]. Tasks that are based on dynamic stimuli elaborate the goal-oriented visual search approach of individuals as they typically are asked to track dynamic stimuli, such as moving target [6, 12, 14, 48, 56, 61,64,67,88,91,106,118,136,139,148–150,165,172,173,175] or video recordings [23, 85, 133, 134, 143].

In contrast, when users authenticate through continuous stimuli, they may not be aware that they are being authenticated, as the stimuli are embedded to everyday tasks, such as reading emails and web browsing [38, 163, 172]. While continuous visual stimuli are of major importance for HCI as they enable unobtrusive authentication, they typically present lower accuracy and it is under-researched field, in comparison to controlled visual stimuli. Research with controlled visual stimuli has focused on refining authentication (e.g., improve accuracy, reduce time) to make implicit gaze-based authentication practical. Understanding the interplay between the diverse factors that influence the controlled-based authentication (e.g., task type, eye tracking metrics, minimum time) would help to move towards feasible and efficient continuous-based authentication.

RESEARCH DIRECTION 4

Blending Authentication with Everyday Tasks

In implicit gaze authentication the user authenticates based on unconscious eye movements when performing a task. So far, most research in the field is based on controlled stimuli. The users are aware that they are going through an authentication task and the same task is used for the enrolment and the recognition phase. Before attempting to move to continuous visual stimuli, it is essential to conduct more research where different stimulus is used for each phase. This is particularly desirable in an everyday settings. It is possible that the required accuracy is achieved by performing multiple tasks. Different tasks may provide better results for different stimuli. A combination of the above could provide the required accuracy for the authentication process. Another approach can be the use of gaze-based features that are task-independent. Another future research direction is to investigate which tasks result in the most useful data for implicit authentication.

Task vs Time as Authentication Factor

Time is important for the acceptance of an authentication mechanisms [51]. Hence, implicit authentication should be performed fast. The majority of the surveyed papers is concerned with tasks as a whole (e.g., [14, 18, 22, 65, 119, 132]), meaning that the authentication process starts after the user has performed one ore more tasks. Time varies from a few seconds (e.g., less than 10 seconds [26, 67], 30 seconds [65], 40 seconds [132]) to a few minutes (e.g., 5 minutes [14], 25 minutes [85]), with tasks that are based on dynamic visual stimuli being faster. To improve performance, tasks can be repeated several times in the same session [46, 135, 152, 165, 175], resulting in longer duration. Very few works consider time as a factor (e.g., time-based analysis [38]). Five seconds seem to be a significant turning point for achieving good accuracy, with dynamic stimuli outperforming static ones [148, 150].

RESEARCH DIRECTION 5

Time as Factor in Implicit Authentication

Authentication is a secondary task for users and needs to be fast and easy. For example, fingerprint authentication is gaining market share because users authenticate in a few seconds. In implicit gaze-based authentication, time is scarcely used as an analysis variable. More systematic research is needed for minimizing the authentication duration while maintaining a high performance, either by performing time series analysis of the authentication or by reducing the duration of the authentication tasks. To do that, there is need to study how performance is interrelated with different task types and visual stimuli, whether authentication can be achieved in less time for certain eye-tracking metrics, whether there is an interrelation between eye-tracking metrics and types of visual stimuli, and whether a combination of certain tasks would enable faster authentication.

How to Evaluate Implicit Gaze-based Authentication

Implicit gaze-based authentication has been evaluated towards *performance*, *security*, *usability*, and *resources consumption*. *Long-term* evaluation studies have also been conducted.

Performance Evaluation

The majority of the works in implicit gaze-based authentication focus on evaluating the proposed schemes towards performance (i.e., efficiency of the classification mechanisms) and explore the efficiency of different features against identification accuracy [26]. Several metrics have been used towards this direction, such as equal error rate – EER (e.g., in [55, 56, 85, 148, 150, 172]), receiver operating characteristic curve – ROC curve (e.g., in [6, 13, 25, 132, 149]), false acceptance rate – FAR (e.g., in [55, 88, 89, 97, 132, 172]), and false rejection rate – FRR (e.g., in [55, 66, 88, 89, 132, 150, 172]).

In the authentication domain, reporting only the accuracy of identification or verification algorithms could conceal critical information about the efficiency of the mechanism and raise serious privacy issues. For example, reporting a 90% accuracy suggests 90% of the attempted users were correctly matched, but does not explain whether the remaining 10% were granted access to the system or not. The used evaluation metrics should assess both the probability of false acceptance and that of false rejection. We underline the importance of adopting the respective ISO/IEC standard for biometric evaluation [59].

When evaluating the performance of identification and verification mechanisms, the sample size is key to ensure the reliability of the obtained results. While in literature several suggestions regarding the sample size of eye tracking studies have been made [40, 116], there are no specific guidelines that have been proposed regarding the implicit gaze-based authentication. The number of participants may vary between less that fifty [14, 150], a few hundreds [21, 28, 131], or even thousands [12]. Moreover, several works are based on publicly available datasets [5, 28, 64, 114, 115, 132, 151, 152] to optimize the identification and verification algorithms. There is to date no gold standard for the sample size when evaluating implicit gaze-based authentication schemes.

Security Evaluation

Security evaluation in implicit gaze-based authentication is most often concerned with impersonation [50, 61, 118, 148, 149, 172] and replay attacks [148, 149]. In impersonation attacks, an adversary tries to fraudulently impersonate a legitimate user. Sluganovic et al. [148] simulated this type of attack and showed that increasing the threshold above which a sample is considered legitimate, decreases the likelihood of falsely accepting but at the same time increases the likelihood of falsely rejecting a legitimate user. Success of such attacks is also related to the stimuli complexity [172] and the type of the attackers: internal attackers (i.e. attackers known to the system) and external attackers (i.e. attackers unknown to the system) [149]. Access to the legitimate user's calibration data also affects the success rate of impersonation attacks [118]. In replay attacks, a valid data transmission is maliciously or fraudulently repeated or delayed. To prevent this type of attacks the visual stimulus shown to the user should never be reused. For example, every time the user starts a new authentication session using a moving dot stimulus, the dot should move to different positions and in different order [148, 149].

Usability and Resources Consumption Evaluation

Very few works focus on evaluating the implicit gaze-based authentication schemes towards usability, such as time efficiency [150] and user experience [150]. Likewise, resources consumption, such as CPU and memory footprint [150] and energy consumption [172], has received little research interest.

Long Term Evaluation

While studying the long-term use is critical for authentication, very few works [6, 92, 118, 150, 173] report such studies. A degradation of accuracy is observed with time regardless of the type of visual stimuli used [92, 150]. To maintain high authentication accuracy, it is necessary to update regularly the owner template. Despite the fact that there is evidence that eye movements change with time [87], the aging factor in not well researched and understood.

RESEARCH DIRECTION 6

Evaluating Gaze-based Implicit Authentication Schemes

Evaluation in implicit gaze-based authentication focus on evaluating the performance of the proposed scheme. There is a research opportunity in expanding the work on security and usability evaluation. This will allow to a) better understand the possible threats of such schemes, b) understand which factors (e.g., stimulus) introduce security vulnerabilities, c) identify the factors that relate to usability and d) study the user acceptance dimension. Implicit gaze-based authentication schemes has only been studied in the lab. Most often the user is instructed to use a chin rest [12, 14, 89, 118, 135] aiming to achieve good calibration and ensure the performance is not a result of inaccurate gaze data. It is possible that a calibration-free gaze cannot provide the required data accuracy for this type of authentication. There is a research opportunity in evaluating such schemes in the wild. This will allow to a) understand how accuracy is influenced in real-life settings, b) study impact of aging effects, c) study impact of learning effects, and d) study different usage contexts.

GAZE-SUPPORTED MULTI-FACTOR AUTHENTICATION

Multi-factor authentication schemes are those that involve two or more authentication factors. The three most common authentication factors are knowledge, possession, and biometric [120]. Eye gaze can be used for supporting either the knowledge factor, by requiring the user to explicitly move their eyes to demonstrate "knowledge" of the authentication pattern, or it can be used for the biometric factor, by processing the user's implicit eye movements to verify their identity. The possession factor refers to authenticating a user by showing they "have" a token, a key, a card, or similar.

Knowledge + Biometric

To outbalance the accuracy issues associated with the some implicit authentication schemes, two-factor authentication schemes were proposed which combine implicit and explicit mechanisms. In this case, an explicit mechanism is used to enter something the user knows, e.g., a PIN, using gaze input, and implicit metrics are collected and analyzed, e.g., angle kappa, to provide additional proof that the user is who they claim to be. Such examples are presented by [54, 124, 140].

In those examples, gaze was utilized for both the knowledge factor and the biometric factor. It is also possible to use gaze as a biometric factor while another modality is used for the knowledge factor. One example is to verify the user's identity through their gaze behavior while they enter a text password using a keyboard or a touchscreen.

It is also feasible to use gaze for the knowledge factor (e.g., enter a PIN by dwelling at digits on an on-screen keypad) while using a different modality for the biometric factor. In that case, the features used in the biometric factor should be passive ones such as the standing posture, facial features, or gait. Otherwise, requiring the user to authenticate via gaze and perform an additional task to collect biometric data could result in very long authentication times. The only work we are aware of that uses gaze input for the knowledge factor, and a non-gaze feature for the biometric factor is SAFE by Boehm et al. [18] where users gazed at a predefined target (knowledge factor) while facial recognition took place (biometric factor).

Knowledge + Possession

Combining explicit gaze-based authentication with a possession factor would also provide an additional layer of security. For example, in GTmoPass [78], the user authenticates at a public display by entering a Gaze-Touch password on their mobile device. Here, the possession factor is the mobile device, while the knowledge factor is the Gaze-Touch password.

Possession + Biometric

We are not aware of works that combined the possession factor and biometric gaze-based authentication. One way this could be done is by requiring the user to provide a physical key in addition to engaging them to a visual task and tracking their eye gaze (e.g., while showing a visual stimuli). This would be more secure than using either alone. For example, this could be used when accessing a door.

GAZE-BASED PRIVACY PROTECTION

While authentication protects privacy indirectly by limiting access to confidential content, some approaches aim at directly protecting private content from attackers. Here, gaze can be leveraged in two ways: a) Actively protecting the user's privacy by, for example, hiding content the user is not looking at, or b) raising the user's awareness of shoulder surfers by detecting the gaze direction of bystanders.

Active Visual Privacy Protection

Eiband et al. [39] showed that while most shoulder surfing resilience research focused on authentication, the vast majority of observed content is text, photos and videos. This means that we need methods to protect the visual privacy of users. Brudy et al. [19] proposed several methods to protect users of public displays from shoulder surfing. The gaze direction of the user and the bystanders were detected using a Kinect device. Privacy protection was done either by moving or hiding content, or by blacking out sensitive content such as personal emails. Ali et al. [7] proposed a slightly similar privacy protection application for detecting bystanders, but they only detected the presence of faces.

Similar systems, like EyeSpot [77] and Private Reader [125], were proposed for privacy protection on mobile devices. In EyeSpot [77], the content that the user is gazing at is visible to them, while the rest is masked either by a black filter overlay, a crystallized mask, or fake content. In the usability analysis of the different filter types, the authors found that the size of the visible spot impacts the reading speed significantly, and that the crystallized filter is more usable compared to the blackout one and fake text in terms of reading speed. The authors found no significant impact of the filters on neither the perceived mental workload nor text comprehension. However, participants favored the crystallized mask as it allowed them to see contextual information such as chat bubbles in chatting apps. Private Reader [125] similarly enhances privacy by rendering the portion of the text that is gazed at. The authors studied the impact on text comprehension and workload, and found that their method reduces comprehension and induces higher workload on attackers compared to the users.

While the aforementioned systems relied on eye gaze to selectively hide or render certain content, other works leveraged the inconspicuous nature of eye gaze to allow privacy-aware interactions. For example, iType [99] allows users to type text on mobile devices using their gaze. Another example is EyeVote [84], which allows users to anonymously vote on public displays without revealing their choices to bystanders. Several systems were proposed for transferring content from public devices to personal ones using eye gaze because it makes it more difficult for bystanders to know which content the user is interested in [110, 158–160].

While these systems were not built with the aim of privacy protection, privacy-aware interactions were a byproduct of using gaze input.

Raising Awareness of Shoulder Surfers in Real Time

In addition to active privacy protection, Brudy et al. [19] also proposed mechanisms for raising the awareness of public display users about bystanders who might be shoulder surfing them. They experimented with flashing the borders of the display when a bystander gazes at the display while it is in use by someone else, and visualizing the passerby's gaze direction and/or body orientation when it is in use.

Zhou et al. [176, 177] proposed multiple interfaces that raise the user's awareness of shoulder surfers through visual and auditory notifications. Similarly, Saad et al. [137] proposed different methods to communicate the presence of shoulder surfers to users by using face recognition. Despite not being based on gaze estimation, these works discuss this as a future step for improving the accuracy of detection and increasing the applicability of their concepts.

RESEARCH DIRECTION 7

Privacy Protection by Assessing Bystander Gaze

Gaze-based privacy protection is a promising application area. However, research done in this area so far is disconnected. Some works investigated how gaze can be used to inform which on-screen content to hide from shoulder surfers [19, 77, 125]. In these works, the presence of shoulder surfers was assumed. Other works studied best practices to inform the user of the presence of shoulder surfers [137, 176, 177]. None of those works studied how to detect the presence of shoulder surfers.

A straight forward idea could be to detect the gaze direction of bystanders to estimate if they are shoulder surfing the user. However, this solution comes with several implications. First, from a technical perspective, wider angle lenses (e.g., fisheye lenses) need to be used, which, however, distort the edges of photos. This raises the challenge of detecting eye contact despite the distortions to the shoulder surfer's face. Second, being able to detect the gaze direction of surrounding bystanders brings its own privacy concerns: Is a user's device allowed to detect the gaze direction of bystanders? How can bystanders consent to that? If consent can be retrieved, would shoulder surfers consent to processing their gaze behavior knowing that this might deter their attacks?

Previous work already discussed how the pervasiveness of eye tracking raises privacy and ethical concerns [73]. Here, we raise an additional concern of how protecting the privacy of the user might result in compromising the privacy of bystanders if we assume that every bystander is an attacker. Addressing this would not only improve privacy protection mechanisms, but can also improve authentication mechanisms. In particular, some observation resilient explicit authentication mechanisms are very effective against shoulder surfing but cannot be used on daily basis due to, for example, requiring long entry times [79]. If the system is aware of the presence of bystanders, it could then require the user to authenticate using a more secure mechanism. This would improve the overall user experience as the user will be using a more usable mechanism.

IMPROVING SECURITY BASED ON GAZE BEHAVIOR

We discussed the use of gaze to support authentication and privacy protection. In addition, tracking the user's gaze behavior can help understand their attitude towards security and detect insecure behavior. A number of attempts to build mechanisms for supporting or improving security have been proposed based on the understanding gained from observing and analyzing user gaze behavior when performing security tasks.

Prior work used eye tracking to study the effectiveness of security indicators on web browsers and the ability of users to detect phishing websites. Here, gaze has not only been used to understand user behavior [9, 29] but also as a mean to improve behavior to prevent such attacks [113]. For example, Arianezhad et al. [9] reported correlations between security expertise and gaze durations at security indicators. While their results highlight the correlation, Miyamoto et al. [113] developed mechanisms to build on this knowledge by proposing a web browser extension preventing users from providing input in web forms until they gazed at the browser's address bar.

Steinfeld et al. used eye tracking to explore users' attitudes towards privacy policies [155]. They revealed users' tendency to read the policy when presented by default, while when given the option to sign their agreement without reading the policy, they tend to skip it. Pfeffel et al. [122] used eye tracking to explore how users decide if an email is phishing email or real.

Rather than for input, some researchers analyzed gaze during authentication with the aim to nudge users towards adopting more secure behavior. Mihajlov et al. [112] explored how much time is spent by users in different registration fields. Similarly, Katsini et al. [69, 71] and Fidas et al. [42] explored where users' attention is drawn and how it is associated with graphical password choices. They used this knowledge to design mechanisms that nudge users towards better password decisions [71, 72]. In graphical authentication, eye tracking data has been used for building dictionaries of hot-spots [96], i.e., frequently selected – and thus insecure – positions and for creating cognition-based user models to provide personalized adaptations of authentication schemes [70, 128].

RESEARCH DIRECTION 8

Understanding Gaze Behavior in Security Tasks

There is relatively little research in this area. Gaze behavior reflects cognitive processes, visual attention, and other user attributes [109] which can be used to identify vulnerabilities of security systems and design improved solutions.

Understanding gaze behavior can help improve security. For example, similar to previous work [9, 29, 113], eye tracking can be used to detect whether or not users examined an email's sender to deter users from accessing links in phishing emails. Another approach is to use gaze to detect fear or sense of urgency [2], which are among the emotions social engineers try to instill in phishing and vishing attacks [130]. Analyzing gaze behavior can also help improve usability and memorability. For example, the user's pupillary response can reflect if the cognitive load induced by recalling passwords is too high, indicating that the scheme's memorability can be improved. Similarly, frequent scanpaths might indicate confusion, which can in turn indicate that the usability of a system or a task (e.g., installing security updates) should be improved.

A drawback of continuous gaze monitoring, even if done with the intention of improving security, is that the tracked gaze data can have negative privacy implications. For example, the widespread use of security applications that leverage gaze data can be a gateway for adversaries to spread malware exploiting the user's gaze data for profiling. We discuss this in detail in "Challenge 2: Privacy Implications of Eye Tracking".

FUTURE CHALLENGES

In the following, we highlight some of the most pressing issues that, in our view, should be addressed in the near future of gaze-based security applications.

Challenge 1: Accuracy and Speed Trade off

Implicit gaze-based security applications require highly accurate gaze estimates to be truly implicit and work without the user's intervention. To collect highly accurate gaze data, calibration is necessary [109]. For a long time, eye trackers required users to be very still and even required them to use chin rests [33]. While modern eye trackers afford to allow users to move around to an extent, they often need to be recalibrated every time the user's or the setup's state change significantly. But calibration introduces an overhead to the interaction process, and it is perceived to be tedious, unnatural and time consuming [164]. There is a lot of research directed at making calibration more of an implicit rather than an explicit procedure by, for example, making it part of the interaction process while reading text or watching videos [81, 123, 156]. Previous work that studied implicit calibration addressed general use cases but not implicit authentication. This leaves room for future work on how to calibrate in a way to optimize the performance of implicit authentication. This requires first understanding the trade-off between calibration time and accuracy in implicit gaze-based authentication.

In contrast, some explicit gaze-based security applications do not require accurate gaze data. For example, many explicit schemes employ calibration-free gaze input methods like gestures [32, 79] and Pursuits [27, 83] which can perform accurately even when using inaccurate gaze data. These techniques require no calibration, as a result of which users can start the authentication process faster. However, calibration-free gaze input techniques often require longer entry times compared to other modalities. For example, in CueAuth [83], users spent 26.35 seconds to authenticate using Pursuits, while touch input required only 3.73 seconds. Achieving a balance between authentication time and calibration time – in particular, while considering the authentication context – is an important direction for future work to maintain fast authentication.

Challenge 2: Privacy Implications of Eye Tracking

The eye tracking technology itself can be a threat to privacy. For example, a user's mobile device with eye tracking enabled could track the eyes of bystanders without their consent. This raises multiple questions. How can bystanders be made aware that a particular user's device can track their eyes? How can their consent be retrieved? And how can their privacy be protected if they do not wish their eyes to be tracked? Like many ubiquitous technologies [95], eye tracking can reveal many private user attributes [100] such as emotional valence [121], mind wandering [162], personality traits [58], and women's hormonal cycles [94]. Another important challenge is to securely store and process the gaze data without leaking it to third parties. This becomes more problematic if the tracking device uploads eye images to the cloud for processing rather than estimating gaze on the fly.

The privacy implications of pervasive eye tracking were discussed in recent work [73], and a few solutions to address this were proposed. For example, PrivacEYE [154] is a system which integrates a mechanical shutter into a wearable eye tracker. The shutter is activated when a bystander's face is in the camera's view. This protects the privacy of bystanders, and assures them that they are not being tracked. Another line of work applied differential privacy to gaze data by introducing noise to gaze data to prevent user identification without compromising the data's utility. Steil et al. [153] applied their differential privacy approach on gaze interfaces in virtual reality, while Liu et al. [101] applied theirs on heat maps. Future HCI research should 1) investigate the privacy implications of pervasive eye tracking, and 2) develop mechanisms for protecting the privacy of not only the users but also everyone in the tracking range such as bystanders.

CONCLUSION

In this paper, we summarize previous work on gaze-based security applications and classify the utility of gaze into: 1) authentication, 2) privacy protection, and 3) understanding gaze behavior in security tasks. We identified eight promising research directions based on gaps that we found in the literature. For example, we see great promise in taking evaluations of explicit and implicit authentication mechanisms to real world settings, there are usability and security benefits of blending authentication with every day tasks, and there is a lack of work on gaze-based privacy protection and gaze behaviour analysis during security tasks. Furthermore, we identified two challenges that are important to address in order to make full use of gaze in security applications and require further research. Namely, there seems to be a trade off between the accuracy and speed of gaze-based security solutions. The trade off is particularly impacted by the need for calibration. A second challenge is that pervasive eye tracking itself can be a threat to privacy of the users of the technology and those around them.

ACKNOWLEDGEMENTS

This work was supported, in part, by the Royal Society of Edinburgh (Award number 65040), and the Deutsche Forschungsgemeinschaft (DFG), Grants AL 1899/2-1 and 1899/4-1.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3751–3763. DOI:http://dx.doi.org/10.1145/3025453.3025461

[2] Yomna Abdelrahman, Anam Ahmad Khan, Joshua Newn, Eduardo Velloso, Sherine Ashraf Safwat, James Bailey, Andreas Bulling, Frank Vetere, and Albrecht Schmidt. 2019. Classifying Attention Types with Thermal Imaging and Eye Tracking. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 3, Article 69 (Sept. 2019), 27 pages. DOI:http://dx.doi.org/10.1145/3351227

[3] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amrl Elmougy. 2019. Just Gaze and Wave: Exploring the Use of Gaze and Gestures for Shoulder-Surfing Resilient Authentication. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19)*. ACM, New York, NY, USA, Article Article 29, 10 pages. DOI: http://dx.doi.org/10.1145/3314111.3319837

[4] Evgeniy R. Abdulin and Oleg V. Komogortsev. 2015. Person Verification via Eye Movement-driven Text Reading Model. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, USA, 1–8. DOI: http://dx.doi.org/10.1109/BTAS.2015.7358786

[5] Narishige Abe, Shigefumi Yamada, and Takashi Shinzaki. 2016. A Novel Local Feature for Eye Movement Authentication. In *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, USA, 1–5. DOI: http://dx.doi.org/10.1109/BIOSIG.2016.7736903

[6] Karan Ahuja, Rahul Islam, Varun Parashar, Kuntal Dey, Chris Harrison, and Mayank Goel. 2018. EyeSpyVR: Interactive Eye Sensing Using Off-the-Shelf, Smartphone-Based VR Headsets. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2, Article 57 (July 2018), 10 pages. DOI:http://dx.doi.org/10.1145/3214260

[7] Mohammed Eunus Ali, Anika Anwar, Ishrat Ahmed, Tanzima Hashem, Lars Kulik, and Egemen Tanin. 2014. Protecting Mobile Users from Visual Privacy Attacks. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 1–4. DOI: http://dx.doi.org/10.1145/2638728.2638788

[8] Hassoumi Almoctar, Pourang Irani, Vsevolod Peysakhovich, and Christophe Hurter. 2018. Path Word: A Multimodal Password Entry Method for Ad-hoc Authentication Based on Digits' Shape and Smooth Pursuit Eye Movements. In *Proceedings of the 20th ACM International Conference on Multimodal Interaction (ICMI '18)*. ACM, New York, NY, USA, 268–277. DOI: http://dx.doi.org/10.1145/3242969.3243008

[9] Majid Arianezhad, L. Jean Camp, Timothy Kelley, and Douglas Stebila. 2013a. Comparative Eye Tracking of Experts and Novices in Web Single Sign-on. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY '13)*. ACM, New York, NY, USA, 105–116. DOI: http://dx.doi.org/10.1145/2435349.2435362

[10] Majid Arianezhad, Douglas Stebila, and Behzad Mozaffari. 2013b. Usability and Security of Gaze-Based Graphical Grid Passwords. In *Financial Cryptography and Data Security*, Andrew A. Adams, Michael Brenner, and Matthew Smith (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 17–33. DOI: http://dx.doi.org/10.1007/978-3-642-41320-9_2

[11] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT '10)*. USENIX Association, Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

[12] Gary Bargary, Jenny M. Bosten, Patrick T. Goodbourn, Adam J. Lawrance-Owen, Ruth E. Hogg, and J.D. Mollon. 2017. Individual Differences in Human Eye Movements: An Oculomotor Signature? *Vision Research* 141 (2017), 157–169. DOI: http://dx.doi.org/10.1016/j.visres.2017.03.001

[13] Akram Bayat and Marc Pomplun. 2018. Biometric Identification Through Eye-Movement Patterns. In *Advances in Human Factors in Simulation and Modeling*, Daniel N. Cassenti (Ed.). Springer International Publishing, Cham, 583–594. DOI: http://dx.doi.org/10.1007/978-3-319-60591-3_53

[14] Roman Bednarik, Tomi Kinnunen, Andrei Mihaila, and Pasi Fränti. 2005. Eye-Movements as a Biometric. In *Image Analysis*, Heikki Kalviainen, Jussi Parkkinen, and Arto Kaarna (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 780–789. DOI: http://dx.doi.org/10.1007/11499145_79

[15] Darrell S. Best and Andrew T. Duchowski. 2016. A Rotary Dial for Gaze-based PIN Entry. In *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications (ETRA '16)*. ACM, New York, NY, USA, 69–76. DOI: http://dx.doi.org/10.1145/2857491.2857527

[16] Ralf Biedert, Mario Frank, Ivan Martinovic, and Dawn Song. 2012. Stimuli for Gaze Based Intrusion Detection. In *Future Information Technology, Application, and Service*, James J. (Jong Hyuk) Park, Victor C.M. Leung, Cho-Li Wang, and Taeshik Shon (Eds.). Springer Netherlands, Dordrecht, 757–763. DOI:http://dx.doi.org/10.1007/978-94-007-4516-2_80

[17] BMW. 2018. BMW camera keeps an eye on the driver. https://www.autonews.com/article/20181001/OEM06/181009966/bmw-camera-keeps-an-eye-on-the-driver. (2018). accessed 19 December 2019.

[18] Arman Boehm, Dongqu Chen, Mario Frank, Ling Huang, Cynthia Kuo, Tihomir Lolic, Ivan Martinovic, and Dawn Song. 2013. SAFE: Secure Authentication with Face and Eyes. In *2013 International Conference on Privacy and Security in Mobile Systems (PRISMS)*. IEEE, USA, 1–8. DOI: http://dx.doi.org/10.1109/PRISMS.2013.6927175

[19] Frederik Brudy, David Ledo, Saul Greenberg, and Andreas Butz. 2014. Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays Through Awareness and Protection. In *Proceedings of The International Symposium on Pervasive Displays (PerDis '14)*. ACM, New York, NY, USA, Article 1, 6 pages. DOI: http://dx.doi.org/10.1145/2611009.2611028

[20] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the Security of Gaze-based Cued-recall Graphical Passwords Using Saliency Masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 3011–3020. DOI: http://dx.doi.org/10.1145/2207676.2208712

[21] Virginio Cantoni, Chiara Galdi, Michele Nappi, Marco Porta, and Daniel Riccio. 2015. GANT: Gaze Analysis Technique for Human Identification. *Pattern Recognition* 48, 4 (2015), 1027–1038. DOI: http://dx.doi.org/10.1016/j.patcog.2014.02.017

[22] Virginio Cantoni, Tomas Lacovara, Marco Porta, and Haochen Wang. 2018. A Study on Gaze-Controlled PIN Input with Biometric Data Analysis. In *Proceedings of the 19th International Conference on Computer Systems and Technologies (CompSysTech '18)*. ACM, New York, NY, USA, 99–103. DOI: http://dx.doi.org/10.1145/3274005.3274029

[23] Dario Cazzato, Marco Leo, Andrea Evangelista, and Cosimo Distante. 2015. Soft Biometrics by Modeling Temporal Series of Gaze Cues Extracted in the Wild. In *Advanced Concepts for Intelligent Vision Systems*, Sebastiano Battiato, Jacques Blanc-Talon, Giovanni Gallo, Wilfried Philips, Dan Popescu, and Paul Scheunders (Eds.). Springer International Publishing, Cham, 391–402. DOI: http://dx.doi.org/10.1007/978-3-319-25903-1_34

[24] Sushil Chauhan, A.S. Arora, and Amit Kaul. 2010. A Survey of Emerging Biometric Modalities. *Procedia Computer Science* 2 (2010), 213–218. DOI: http://dx.doi.org/10.1016/j.procs.2010.11.027

[25] Elena N. Cherepovskaya and Andrey V. Lyamin. 2017. An Evaluation of Biometrie Identification Approach on Low-frequency Eye Tracking Data. In *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. IEEE, USA, 123–128. DOI: http://dx.doi.org/10.1109/SAMI.2017.7880288

[26] Nguyen Viet Cuong, Vu Dinh, and Lam Si Tung Ho. 2012. Mel-frequency Cepstral Coefficients for Eye Movement Identification. In *2012 IEEE 24th International Conference on Tools with Artificial Intelligence*. IEEE, USA, 253–260. DOI: http://dx.doi.org/10.1109/ICTAI.2012.42

[27] Dietlind Helene Cymek, Antje Christine Venjakob, Stefan Ruff, Otto Hans-Martin Lutz, Simon Hofmann, and Matthias Roetting. 2014. Entering PIN Codes by Smooth Pursuit Eye Movements. *Journal of Eye Movement Research* 7, 4, Article 1 (2014), 11 pages. DOI:http://dx.doi.org/10.16910/jemr.7.4.1

[28] Antitza Dantcheva, Nesli Erdogmus, and Jean-Luc Dugelay. 2011. On The Reliability of Eye Color as a Soft Biometric Trait. In *2011 IEEE Workshop on Applications of Computer Vision (WACV)*. IEEE, USA, 227–231. DOI: http://dx.doi.org/10.1109/WACV.2011.5711507

[29] Ali Darwish and Emad Bataineh. 2012. Eye Tracking Analysis of Browser Security Indicators. In *2012 International Conference on Computer Systems and Industrial Informatics*. IEEE, USA, 1–6. DOI: http://dx.doi.org/10.1109/ICCSII.2012.6454330

[30] Ali Darwish and Michel Pasquier. 2013. Biometric Identification Using the Dynamic Features of the Eyes. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, USA, 1–6. DOI: http://dx.doi.org/10.1109/BTAS.2013.6712724

[31] Nigel Davies, Sarah Clinch, and Florian Alt. 2014. Pervasive Displays: Understanding the Future of Digital Signage. *Synthesis Lectures on Mobile and Pervasive Computing* 8, 1 (Apr. 2014), 1–128. DOI: http://dx.doi.org/10.2200/s00558ed1v01y201312mpc011

[32] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into My Eyes!: Can You Guess My Password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. DOI: http://dx.doi.org/10.1145/1572532.1572542

[33] Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of Eye-gaze Interaction Methods for Security Enhanced PIN-entry. In *Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces (OZCHI '07)*. ACM, New York, NY, USA, 199–202. DOI: http://dx.doi.org/10.1145/1324892.1324932

[34] Alexander De Luca, Roman Weiss, Heinrich Hussmann, and Xueli An. 2008. Eyepass - Eye-stroke Authentication for Public Terminals. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems (CHI EA '08)*. ACM, New York, NY, USA, 3003–3008. DOI: http://dx.doi.org/10.1145/1358628.1358798

[35] Heiko Drewes, Mohamed Khamis, and Florian Alt. 2019. DialPlates:Enabling Pursuits-based User Interfaces with Large Target Numbers. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia (MUM '19)*. ACM, New York, NY, USA, Article Article 10, 10 pages. DOI: http://dx.doi.org/10.1145/3365610.3365626

[36] Heiko Drewes and Albrecht Schmidt. 2007. Interacting with the Computer Using Gaze Gestures. In *Human-Computer Interaction – INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II*, Cécilia Baranauskas, Philippe Palanque, Julio Abascal, and Simone Diniz Junqueira Barbosa (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 475–488. DOI: http://dx.doi.org/10.1007/978-3-540-74800-7_43

[37] Paul Dunphy, Andrew Fitch, and Patrick Olivier. 2008. Gaze-contingent Passwords at the ATM. In *4th Conference on Communication by Gaze Interaction (COGAIN)*. COGAIN, Prague,Czech Republic, 59–62.

[38] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. 2016. Looks Like Eve: Exposing Insider Threats Using Eye Movement Biometrics. *ACM Transactions on Privacy and Security* 19, 1, Article 1 (June 2016), 31 pages. DOI: http://dx.doi.org/10.1145/2904018

[39] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 4254–4265. DOI: http://dx.doi.org/10.1145/3025453.3025636

[40] Sukru Eraslan, Yeliz Yesilada, and Simon Harper. 2016. Eye Tracking Scanpath Analysis on Web Pages: How Many Users?. In *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications (ETRA '16)*. ACM, New York, NY, USA, 103–110. DOI: http://dx.doi.org/10.1145/2857491.2857519

[41] Nastaran Maus Esfahani. 2016. A Brief Review of Human Identification Using Eye Movement. *Journal of Pattern Recognition Research* 11, 1 (2016), 15–24. DOI:http://dx.doi.org/10.13176/11.705

[42] Christos Fidas, Marios Belk, George Hadjidemetriou, and Andreas Pitsillides. 2019. Influences of Mixed Reality and Human Cognition on Picture Passwords: An Eye Tracking Study. In *Human-Computer Interaction – INTERACT 2019*, David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris (Eds.). Springer International Publishing, Cham, 304–313. DOI:http://dx.doi.org/10.1007/978-3-030-29384-0_19

[43] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010a. Input Precision for Gaze-based Graphical Passwords. In *CHI '10 Extended Abstracts on Human Factors in Computing Systems (CHI EA '10)*. ACM, New York, NY, USA, 4279–4284. DOI: http://dx.doi.org/10.1145/1753846.1754139

[44] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010b. Shoulder-surfing Resistance with Eye-gaze Entry in Cued-recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1107–1110. DOI: http://dx.doi.org/10.1145/1753326.1753491

[45] Wolfgang Fuhl, Marc Tonsen, Andreas Bulling, and Enkelejda Kasneci. 2016. Pupil Detection for Head-mounted Eye Tracking in the Wild: An Evaluation of the State of the Art. *Machine Vision and Applications* 27, 8 (Nov 2016), 1275–1288. DOI: http://dx.doi.org/10.1007/s00138-016-0776-4

[46] Chiara Galdi, Michele Nappi, Daniel Riccio, Virginio Cantoni, and Marco Porta. 2013. A New Gaze Analysis Based Soft-Biometric. In *Pattern Recognition*, Jesús Ariel Carrasco-Ochoa, José Francisco Martínez-Trinidad, Joaquín Salas Rodríguez, and Gabriella Sanniti di Baja (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 136–144. DOI: http://dx.doi.org/10.1007/978-3-642-38989-4_14

[47] Chiara Galdi, Michele Nappi, Daniel Riccio, and Harry Wechsler. 2016. Eye Movement Analysis for Human Authentication: A Critical Survey. *Pattern Recognition Letters* 84 (2016), 272–283. DOI: http://dx.doi.org/10.1016/j.patrec.2016.11.002

[48] Anjith George and Aurobinda Routray. 2016. A Score Level Fusion method for Eye Movement Biometrics. *Pattern Recognition Letters* 82 (2016), 207–215. DOI: http://dx.doi.org/10.1016/j.patrec.2015.11.020

[49] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. 2019. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, USA, 277–285. DOI: http://dx.doi.org/10.1109/VR.2019.8797862

[50] Isaac Griswold-Steiner, Zakery Fyke, Mushfique Ahmed, and Abdul Serwadda. 2018. Morph-a-Dope: Using Pupil Manipulation to Spoof Eye Movement Biometrics. In *2018 9th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*. IEEE, USA, 543–552. DOI: http://dx.doi.org/10.1109/UEMCON.2018.8796625

[51] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 4806–4817. DOI: http://dx.doi.org/10.1145/2858036.2858267

[52] Teresa Hirzle, Jan Gugenheimer, Florian Geiselhart, Andreas Bulling, and Enrico Rukzio. 2019. A Design Space for Gaze Interaction on Head-mounted Displays. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 625, 12 pages. DOI: http://dx.doi.org/10.1145/3290605.3300855

[53] Bogdan Hoanca and Kenrick Mock. 2006. Secure Graphical Password System for High Traffic Public Areas. In *Proceedings of the 2006 Symposium on Eye Tracking Research & Applications (ETRA '06)*. ACM, New York, NY, USA, 35–35. DOI: http://dx.doi.org/10.1145/1117309.1117319

[54] Bogdan Hoanca and Kenrick Mock. 2011. Methods and Systems for Multiple Factor Authentication using Gaze Tracking and Iris Scanning. (July 2011). https://patents.google.com/patent/US7986816B1 US Patent 7,986,816.

[55] Corey D. Holland and Oleg V. Komogortsev. 2011. Biometric Identification via Eye Movement Scanpaths in Reading. In *2011 International Joint Conference on Biometrics (IJCB)*. IEEE, USA, 1–8. DOI: http://dx.doi.org/10.1109/IJCB.2011.6117536

[56] Corey D. Holland and Oleg V. Komogortsev. 2012. Biometric Verification via Complex Eye Movements: The Effects of Environment and Stimulus. In *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, USA, 39–46. DOI: http://dx.doi.org/10.1109/BTAS.2012.6374556

[57] Corey D. Holland and Oleg V. Komogortsev. 2013. Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus. *IEEE Transactions on Information Forensics and Security* 8, 12 (Dec 2013), 2115–2126. DOI: http://dx.doi.org/10.1109/TIFS.2013.2285884

[58] Sabrina Hoppe, Tobias Loetscher, Stephanie A. Morey, and Andreas Bulling. 2018. Eye Movements During Everyday Behavior Predict Personality Traits. *Frontiers in Human Neuroscience* 12 (Apr 2018), 1–8. DOI:http://dx.doi.org/10.3389/fnhum.2018.00105

[59] ISO/IEC 19795-1:2006 2006. *Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. Standard. International Organization for Standardization, Geneva, CH.

[60] Robert J. K. Jacob. 1990. What You Look at is What You Get: Eye Movement-based Interaction Techniques. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '90)*. ACM, New York, NY, USA, 11–18. DOI: http://dx.doi.org/10.1145/97243.97246

[61] Martti Juhola, Youming Zhang, and Jyrki Rasku. 2013. Biometric Verification of a Subject through Eye Movements. *Computers in Biology and Medicine* 43, 1 (2013), 42–50. DOI: http://dx.doi.org/10.1016/j.compbiomed.2012.10.005

[62] Paweł Kasprowski. 2013. The Impact of Temporal Proximity between Samples on Eye Movement Biometric Identification. In *Computer Information Systems and Industrial Management*, Khalid Saeed, Rituparna Chaki, Agostino Cortesi, and Sławomir Wierzchoń (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 77–87. DOI: http://dx.doi.org/10.1007/978-3-642-40925-7_8

[63] Paweł Kasprowski and Katarzyna Harężlak. 2014. Cheap and Easy PIN Entering Using Eye Gaze. *Annales Universitatis Mariae Curie-Skłodowska. Sectio AI, Informatica* 14, 1 (2014), 75–84.

[64] Paweł Kasprowski and Katarzyna Harężlak. 2016. Using Dissimilarity Matrix for Eye Movement Biometrics with a Jumping Point Experiment. In *Intelligent Decision Technologies 2016*, Ireneusz Czarnowski, Alfonso Mateos Caballero, Robert J. Howlett, and Lakhmi C. Jain (Eds.). Springer International Publishing, Cham, 83–93. DOI: http://dx.doi.org/10.1007/978-3-319-39627-9_8

[65] Paweł Kasprowski and Katarzyna Harężlak. 2018a. Biometric Identification Using Gaze and Mouse Dynamics During Game Playing. In *Beyond Databases, Architectures and Structures. Facing the Challenges of Data Proliferation and Growing Variety*, Stanisław Kozielski, Dariusz Mrozek, Paweł Kasprowski, Bożena Małysiak-Mrozek, and Daniel Kostrzewa (Eds.). Springer International Publishing, Cham, 494–504. DOI:http://dx.doi.org/10.1007/978-3-319-99987-6_38

[66] Paweł Kasprowski and Katarzyna Harężlak. 2018b. Fusion of Eye Movement and Mouse Dynamics for Reliable Behavioral Biometrics. *Pattern Analysis and Applications* 21, 1 (Feb 2018), 91–103. DOI: http://dx.doi.org/10.1007/s10044-016-0568-5

[67] Paweł Kasprowski and Józef Ober. 2004. Eye Movements in Biometrics. In *Biometric Authentication*, Davide Maltoni and Anil K. Jain (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 248–258. DOI: http://dx.doi.org/10.1007/978-3-540-25976-3_23

[68] Moritz Kassner, William Patera, and Andreas Bulling. 2014. Pupil: An Open Source Platform for Pervasive Eye Tracking and Mobile Gaze-based Interaction. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 1151–1160. DOI: http://dx.doi.org/10.1145/2638728.2641695

[69] Christina Katsini, Christos Fidas, Marios Belk, George Samaras, and Nikolaos Avouris. 2019. A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication. *International Journal of Human-Computer Interaction* 25, 19 (2019), 1800–1812. DOI: http://dx.doi.org/10.1080/10447318.2019.1574057

[70] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018a. Eye Gaze-Driven Prediction of Cognitive Differences during Graphical Password Composition. In *23rd International Conference on Intelligent User Interfaces (IUI '18)*. ACM, New York, NY, USA, 147–152. DOI: http://dx.doi.org/10.1145/3172944.3172996

[71] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018b. Influences of Human Cognition and Visual Behavior on Password Strength During Picture Password Composition. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 87, 14 pages. DOI: http://dx.doi.org/10.1145/3173574.3173661

[72] Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018c. Towards Gaze-based Quantification of the Security of Graphical Authentication Schemes. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications (ETRA '18)*. ACM, New York, NY, USA, Article 17, 5 pages. DOI: http://dx.doi.org/10.1145/3204493.3204589

[73] Mohamed Khamis, Florian Alt, and Andreas Bulling. 2018. The Past, Present, and Future of Gaze-enabled Handheld Mobile Devices: Survey and Lessons Learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '18)*. ACM, New York, NY, USA, Article Article 38, 17 pages. DOI:http://dx.doi.org/10.1145/3229434.3229452

[74] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2156–2164. DOI: http://dx.doi.org/10.1145/2851581.2892314

[75] Mohamed Khamis, Anita Baier, Niels Henze, Florian Alt, and Andreas Bulling. 2018. Understanding Face and Eye Visibility in Front-Facing Cameras of Smartphones Used in the Wild. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 280, 12 pages. DOI: http://dx.doi.org/10.1145/3173574.3173854

[76] Mohamed Khamis, Linda Bandelow, Stina Schick, Dario Casadevall, Andreas Bulling, and Florian Alt. 2017. They Are All After You: Investigating the Viability of A Threat Model That Involves Multiple Shoulder Surfers. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia (MUM '17)*. ACM, New York, NY, USA, 31–35. DOI: http://dx.doi.org/10.1145/3152832.3152851

[77] Mohamed Khamis, Malin Eiband, Martin ZÃijrn, and Heinrich Hussmann. 2018. EyeSpot: Leveraging Gaze to Protect Private Text Content on Mobile Devices from Shoulder Surfing. *Multimodal Technologies and Interaction* 2, 3, Article 45 (2018), 15 pages. DOI: http://dx.doi.org/10.3390/mti2030045

[78] Mohamed Khamis, Regina Hasholzner, Andreas Bulling, and Florian Alt. 2017a. GTmoPass: Two-factor Authentication on Public Displays Using GazeTouch passwords and Personal Mobile Devices. In *Proceedings of the 6th International Symposium on Pervasive Displays (PerDis '17)*. ACM, New York, NY, USA, Article Article 8, 9 pages. DOI: http://dx.doi.org/10.1145/3078810.3078815

[79] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017b. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction (ICMI 2017)*. ACM, New York, NY, USA, 446–450. DOI: http://dx.doi.org/10.1145/3136755.3136809

[80] Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. 2018. VRPursuits: Interaction in Virtual Reality using Smooth Pursuit Eye Movements. In *Proceedings of the 2018 International Conference on Advanced Visual Interfaces (AVI '18)*. ACM, New York, NY, USA, Article Article 18, 8 pages. DOI: http://dx.doi.org/10.1145/3206505.3206522

[81] Mohamed Khamis, Ozan Saltuk, Alina Hang, Katharina Stolz, Andreas Bulling, and Florian Alt. 2016. TextPursuits: Using Text for Pursuits-based Interaction and Calibration on Public Displays. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16)*. ACM, New York, NY, USA, 274–285. DOI:http://dx.doi.org/10.1145/2971648.2971679

[82] Mohamed Khamis, Tobias Seitz, Leonhard Mertl, Alice Nguyen, Mario Schneller, and Zhe Li. 2019. Passquerade: Improving Error Correction of Text Passwords on Mobile Devices by Using Graphic Filters for Password Masking. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 686, 8 pages. DOI: http://dx.doi.org/10.1145/3290605.3300916

[83] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4, Article 174 (Dec. 2018), 22 pages. DOI:http://dx.doi.org/10.1145/3287052

[84] Mohamed Khamis, Ludwig Trotter, Markus Tessmann, Christina Dannhart, Andreas Bulling, and Florian Alt. 2016. EyeVote in the Wild: Do Users Bother Correcting System Errors on Public Displays?. In *Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia (MUM '16)*. ACM, New York, NY, USA, 57–62. DOI: http://dx.doi.org/10.1145/3012709.3012743

[85] Tomi Kinnunen, Filip Sedlak, and Roman Bednarik. 2010. Towards Task-independent Person Authentication Using Eye Movement Signals. In *Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications (ETRA '10)*. ACM, New York, NY, USA, 187–190. DOI: http://dx.doi.org/10.1145/1743666.1743712

[86] Tomasz Kocejko and Jerzy Wtorek. 2012. Gaze Pattern Lock for Elders and Disabled. In *Information Technologies in Biomedicine*, Ewa Piętka and Jacek Kawa (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 589–602. DOI: http://dx.doi.org/10.1007/978-3-642-31196-3_59

[87] Oleg V. Komogortsev, Corey D. Holland, and Alex Karpov. 2014. Template Aging in Eye Movement-driven Biometrics. In *Biometric and Surveillance Technology for Human and Activity Identification XI*, Vol. 9075. SPIE, USA, Article 90750A, 9 pages. DOI: http://dx.doi.org/10.1117/12.2050594

[88] Oleg V. Komogortsev, Sampath Jayarathna, Cecilia R. Aragon, and Mechehoul Mahmoud. 2010. Biometric Identification via an Oculomotor Plant Mathematical Model. In *Proceedings of the 2010 Symposium on Eye-Tracking Research & Applications (ETRA '10)*. ACM, New York, NY, USA, 57–60. DOI: http://dx.doi.org/10.1145/1743666.1743679

[89] Oleg V. Komogortsev, Alexey Karpov, and Corey D. Holland. 2012a. CUE: Counterfeit-resistant Usable Eye Movement-based Authentication via Oculomotor Plant Characteristics and Complex Eye Movement Patterns. In *Sensing Technologies for Global Health, Military Medicine, Disaster Response, and Environmental Monitoring II; and Biometric Technology for Human Identification IX*, Vol. 8371. SPIE, USA, Article 83711X, 9 pages. DOI: http://dx.doi.org/10.1117/12.919219

[90] Oleg V. Komogortsev, Alexey Karpov, Corey D. Holland, and Hugo P. Proença. 2012b. Multimodal Ocular Biometrics Approach: A Feasibility Study. In *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, USA, 209–216. DOI: http://dx.doi.org/10.1109/BTAS.2012.6374579

[91] Oleg V. Komogortsev, Alex Karpov, Larry R. Price, and Cecilia R. Aragon. 2012. Biometric authentication via oculomotor plant characteristics. In *2012 5th IAPR International Conference on Biometrics (ICB)*. IEEE, USA, 413–420. DOI: http://dx.doi.org/10.1109/ICB.2012.6199786

[92] Oleg V. Komogortsev and Ioannis Rigas. 2015. BioEye 2015: Competition on Biometrics via Eye Movements. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, USA, 1–8. DOI: http://dx.doi.org/10.1109/BTAS.2015.7358750

[93] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing Shoulder-surfing by Using Gaze-based Password Entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. ACM, New York, NY, USA, 13–19. DOI: http://dx.doi.org/10.1145/1280680.1280683

[94] Bruno Laeng and Liv Falkenberg. 2007. Women's Pupillary Responses to Sexually Significant Others During the Hormonal Cycle. *Hormones and Behavior* 52, 4 (Nov. 2007), 520–530. DOI: http://dx.doi.org/10.1016/j.yhbeh.2007.07.013

[95] Marc Langheinrich. 2009. Privacy in Ubiquitous Computing. In *Ubiquitous Computing Fundamentals*, John Krumm (Ed.). Chapman & Hall / CRC, NW, USA.

[96] Daniel LeBlanc, Alain Forget, and Robert Biddle. 2010. Guessing Click-based Graphical Passwords by Eye Tracking. In *2010 Eighth International Conference on Privacy, Security and Trust*. IEEE, USA, 197–204. DOI:http://dx.doi.org/10.1109/PST.2010.5593249

[97] Chunyong Li, Jiguo Xue, Cheng Quan, Jingwei Yue, and Chenggang Zhang. 2018. Biometric Recognition via Texture Features of Eye Movement Trajectories in a Visual Searching Task. *PLOS ONE* 13, 4 (Apr 2018), 1–24. DOI: http://dx.doi.org/10.1371/journal.pone.0194475

[98] Na Li, Qianhong Wu, Jingwen Liu, Wei Hu, Bo Qin, and Wei Wu. 2017b. EyeSec: A Practical Shoulder-Surfing Resistant Gaze-Based Authentication System. In *Information Security Practice and Experience*, Joseph K. Liu and Pierangela Samarati (Eds.). Springer International Publishing, Cham, 435–453. DOI: http://dx.doi.org/10.1007/978-3-319-72359-4_26

[99] Zhenjiang Li, Mo Li, Prasant Mohapatra, Jinsong Han, and Shuaiyu Chen. 2017a. iType: Using Eye Gaze to Enhance Typing Privacy. In *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. IEEE, USA, 1–9. DOI: http://dx.doi.org/10.1109/INFOCOM.2017.8057233

[100] Daniel J. Liebling and Sören Preibusch. 2014. Privacy Considerations for a Pervasive Eye Tracking World. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 1169–1177. DOI: http://dx.doi.org/10.1145/2638728.2641688

[101] Ao Liu, Lirong Xia, Andrew Duchowski, Reynold Bailey, Kenneth Holmqvist, and Eakta Jain. 2019. Differential Privacy for Eye-tracking Data. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19)*. ACM, New York, NY, USA, Article 28, 10 pages. DOI: http://dx.doi.org/10.1145/3314111.3319823

[102] Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang. 2015. Exploiting Eye Tracking for Smartphone Authentication. In *Applied Cryptography and Network Security*, Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis (Eds.). Springer International Publishing, Cham, 457–477. DOI: http://dx.doi.org/10.1007/978-3-319-28166-7_22

[103] Su Liu, John D. Wilson, and Yin Xia. 2017. Eye Gazing Passcode Generation Crossing Augmented Reality (AR) and Virtual Reality (VR) Devices. (Nov. 2017). https://patents.google.com/patent/US9824206B1 US Patent 9,824,206.

[104] Andrey V. Lyamin and Elena N. Cherepovskaya. 2015. Biometric Student Identification Using Low-frequency Eye Tracker. In *2015 9th International Conference on Application of Information and Communication Technologies (AICT)*. IEEE, Red Hook, NY, USA, 191–195. DOI: http://dx.doi.org/10.1109/ICAICT.2015.7338544

[105] Andrey V. Lyamin and Elena N. Cherepovskaya. 2017. An Approach to Biometric Identification by Using Low-Frequency Eye Tracker. *IEEE Transactions on Information Forensics and Security* 12, 4 (April 2017), 881–891. DOI: http://dx.doi.org/10.1109/TIFS.2016.2639342

[106] Zhuo Ma, Xinglong Wang, Ruijie Ma, Zhuzhu Wang, and Jianfeng Ma. 2018. Integrating Gaze Tracking and Head-Motion Prediction for Mobile Device Authentication: A Proof of Concept. *Sensors* 18, 9 (Aug 2018), 2894. DOI: http://dx.doi.org/10.3390/s18092894

[107] Anthony J. Maeder and Clinton B. Fookes. 2003. A Visual Attention Approach to Personal Identification. In *Eighth Australian and New Zealand Intelligent Information Systems Conference (ANZIIS 2003)*. The Australian Pattern Recognition Society, Brisbane, QLD, 55–60. https://eprints.qut.edu.au/17897

[108] Anthony J. Maeder, Clinton B. Fookes, and Sridha Sridharan. 2004. Gaze Based User Authentication for Personal Computer Applications. In *Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004*. IEEE, USA, 727–730. DOI: http://dx.doi.org/10.1109/ISIMP.2004.1434167

[109] Päivi Majaranta and Andreas Bulling. 2014. Eye Tracking and Eye-Based Human–Computer Interaction. In *Advances in Physiological Computing*, Stephen H. Fairclough and Kiel Gilleade (Eds.). Springer London, London, 39–65. DOI: http://dx.doi.org/10.1007/978-1-4471-6392-3_3

[110] Ville Mäkelä, Mohamed Khamis, Lukas Mecke, Jobin James, Markku Turunen, and Florian Alt. 2018. Pocket Transfers: Interaction Techniques for Transferring Content from Situated Displays to Mobile Devices.. In *Proceedings of the 36th Annual ACM Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article Paper 135, 13 pages. DOI: http://dx.doi.org/10.1145/3173574.3173709

[111] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou. 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys Tutorials* 17, 3 (2015), 1268–1293. DOI: http://dx.doi.org/10.1109/COMST.2014.2386915

[112] Martin Mihajlov, Marija Trpkova, and Sime Arsenovski. 2013. Eye Tracking Recognition-based Graphical Authentication. In *2013 7th International Conference on Application of Information and Communication Technologies*. IEEE, USA, 1–5. DOI: http://dx.doi.org/10.1109/ICAICT.2013.6722632

[113] Daisuke Miyamoto, Takuji Iimura, Gregory Blanc, Hajime Tazaki, and Youki Kadobayashi. 2014. EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits. In *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*. IEEE, USA, 56–65. DOI: http://dx.doi.org/10.1109/BADGERS.2014.14

[114] Mohammad Reza Mahmoudian Motlagh and Patrick Bours. 2014. User Identification Based on Eye Gaze Data. In *Proceedings of Norwegian Information Security Conference 2014 (NISK 2014)*. Trondheim: Akademika, Trondheim, Norway, 1–9.

[115] Subhadeep Mukhopadhyay and Shinjini Nandi. 2018. LPiTrack: Eye Movement Pattern Recognition Algorithm and Application to Biometric Identification. *Machine Learning* 107, 2 (Feb 2018), 313–331. DOI: http://dx.doi.org/10.1007/s10994-017-5649-1

[116] Jakob Nielsen and Kara Pernice. 2010. *Eye Tracking Web Usability*. New Riders, Berkeley, CA, USA.

[117] Ishan Nigam, Mayank Vatsa, and Richa Singh. 2015. Ocular Biometrics: A Survey of Modalities and Fusion Approaches. *Information Fusion* 26 (2015), 1–35. DOI: http://dx.doi.org/10.1016/j.inffus.2015.03.005

[118] Masakatsu Nishigaki and Daisuke Arai. 2008. A User Authentication based on Human Reflexes using Blind Spot and Saccade Response. *International Journal of Biometrics* 1, 2 (2008), 173–190. DOI: http://dx.doi.org/10.1504/IJBM.2008.020143

[119] Nahumi Nugrahaningsih and Marco Porta. 2014. Pupil Size as a Biometric Trait. In *Biometric Authentication*, Virginio Cantoni, Dimo Dimov, and Massimo Tistarelli (Eds.). Springer International Publishing, Cham, 222–233. DOI: http://dx.doi.org/10.1007/978-3-319-13386-7_18

[120] Lawrence O'Gorman. 2003. Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proc. IEEE* 91, 12 (Dec 2003), 2021–2040. DOI: http://dx.doi.org/10.1109/JPROC.2003.819611

[121] Timo Partala, Maria Jokiniemi, and Veikko Surakka. 2000. Pupillary Responses to Emotionally Provocative Stimuli. In *Proceedings of the 2000 Symposium on Eye Tracking Research & Applications (ETRA '00)*. ACM, New York, NY, USA, 123–129. DOI: http://dx.doi.org/10.1145/355017.355042

[122] Kevin Pfeffel, Philipp Ulsamer, and Nicholas H. Müller. 2019. Where the User Does Look When Reading Phishing Mails – An Eye-Tracking Study. In *Learning and Collaboration Technologies. Designing Learning Experiences*, Panayiotis Zaphiris and Andri Ioannou (Eds.). Springer International Publishing, Cham, 277–287. DOI: http://dx.doi.org/10.1007/978-3-030-21814-0_21

[123] Ken Pfeuffer, Melodie Vidal, Jayson Turner, Andreas Bulling, and Hans Gellersen. 2013. Pursuit Calibration: Making Gaze Calibration Less Tedious and More Flexible. In *Proceedings of the 26th Annual ACM Symposium on User Interface Software and Technology (UIST '13)*. ACM, New York, NY, USA, 261–270. DOI:http://dx.doi.org/10.1145/2501988.2501998

[124] Carlos-Alberto Quintana-Nevárez, Francisco López-Orozco, and Rogelio Florencia-Juárez. 2017. Biometric authentication based on eye movements by using scan-path comparison algorithms. In *Proceedings of the RCCS-SPIDTEC2 Workshop on International Regional Consortium for Foundations, Research and Spread of Emerging Technologies in Computing Sciences*, Vol. 2031. CEUR-WS, Hannover, Germany, 33–38. http://ceur-ws.org/Vol-2031/p5.pdf

[125] Kirill Ragozin, Yun Suen Pai, Olivier Augereau, Koichi Kise, Jochen Kerdels, and Kai Kunze. 2019. Private Reader: Using Eye Tracking to Improve Reading Privacy in Public Spaces. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '19)*. ACM, New York, NY, USA, Article Article 18, 6 pages. DOI: http://dx.doi.org/10.1145/3338286.3340129

[126] Vijay Rajanna, Adil H. Malla, Rahul A. Bhagat, and Tracy Hammond. 2018. DyGazePass: A Gaze Gesture-based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attacks. In *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*. IEEE, USA, 1–8. DOI: http://dx.doi.org/10.1109/ISBA.2018.8311458

[127] Vijay Rajanna, Seth Polsley, Paul Taele, and Tracy Hammond. 2017. A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. ACM, New York, NY, USA, 1978–1986. DOI: http://dx.doi.org/10.1145/3027063.3053070

[128] George E. Raptis, Christina Katsini, Marios Belk, Christos Fidas, George Samaras, and Nikolaos Avouris. 2017. Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles: Method and Feasibility Studies. In *Proceedings of the 25th Conference on User Modeling, Adaptation and Personalization (UMAP '17)*. ACM, New York, NY, USA, 164–173. DOI:http://dx.doi.org/10.1145/3079628.3079690

[129] Real User. 2005. Passfaces: Two Factor Authentication for the Enterprise. Webpage. (2005). http://www.realuser.com/ Retrieved August 20, 2019.

[130] Karen Renaud and Merrill Warkentin. 2017. Using Intervention Mapping to Breach the Cyber-defense Deficit. In *Proceedings of the 12th Annual Symposium on Information Assurance (ASIA'17)*. 14–22.

[131] Ioannis Rigas, Evgeniy Abdulin, and Oleg V. Komogortsev. 2016. Towards a Multi-source Fusion Approach for Eye Movement-driven Recognition. *Information Fusion* 32 (2016), 13–25. DOI: http://dx.doi.org/10.1016/j.inffus.2015.08.003 SI: Information Fusion in Biometrics.

[132] Ioannis Rigas, George Economou, and Spiros Fotopoulos. 2012. Biometric Identification Based on the Eye Movements and Graph Matching Techniques. *Pattern Recognition Letters* 33, 6 (2012), 786–792. DOI:http://dx.doi.org/10.1016/j.patrec.2012.01.003

[133] Ioannis Rigas and Oleg V. Komogortsev. 2014a. Biometric Recognition via Fixation Density Maps. In *Biometric and Surveillance Technology for Human and Activity Identification XI*, Ioannis A. Kakadiaris, Walter J. Scheirer, and Christoph Busch (Eds.), Vol. 9075. International Society for Optics and Photonics, SPIE, USA, 154–163. DOI: http://dx.doi.org/10.1117/12.2054227

[134] Ioannis Rigas and Oleg V. Komogortsev. 2014b. Biometric Recognition via Probabilistic Spatial Projection of Eye Movement Trajectories in Dynamic Visual Environments. *IEEE Transactions on Information Forensics and Security* 9, 10 (Oct 2014), 1743–1754. DOI: http://dx.doi.org/10.1109/TIFS.2014.2350960

[135] Ioannis Rigas, Oleg V. Komogortsev, and Reza Shadmehr. 2016. Biometric Recognition via Eye Movements: Saccadic Vigor and Acceleration Cues. *ACM Transactions on Applied Perception* 13, 2, Article 6 (Jan. 2016), 21 pages. DOI: http://dx.doi.org/10.1145/2842614

[136] Jamison Rose, Yudong Liu, and Ahmed Awad. 2017. Biometric Authentication Using Mouse and Eye Movement Data. *Journal of Cyber Security and Mobility* 6, 1 (2017), 1–16. DOI: http://dx.doi.org/10.13052/jcsm2245-1439.611

[137] Alia Saad, Michael Chukwu, and Stefan Schneegass. 2018. Communicating Shoulder Surfing Attacks to Users. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (MUM 2018)*. ACM, New York, NY, USA, 147–152. DOI:http://dx.doi.org/10.1145/3282894.3282919

[138] Usman Saeed. 2014. A Survey Of Automatic Person Recognition Using Eye Movements. *International Journal of Pattern Recognition and Artificial Intelligence* 28, 08 (2014), 1456015:1–1456015:21. DOI:http://dx.doi.org/10.1142/S0218001414560151

[139] Usman Saeed. 2016. Eye Movements During Scene Understanding for Biometric Identification. *Pattern Recognition Letters* 82 (2016), 190–195. DOI: http://dx.doi.org/10.1016/j.patrec.2015.06.019 SI: An Insight on Eye Biometrics.

[140] Daiki Sakai, Michiya Yamamoto, Takashi Nagamatsu, and Satoshi Fukumori. 2016. Enter Your PIN Code Securely!: Utilization of Personal Difference of Angle Kappa. In *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications (ETRA '16)*. ACM, New York, NY, USA, 317–318. DOI:http://dx.doi.org/10.1145/2857491.2884059

[141] Hananeh Salehifar, Peyman Bayat, and Mojtaba Amiri Majd. 2019. Eye Gesture Blink Password: A New Authentication System with High Memorable and Maximum Password Length. *Multimedia Tools and Applications* 78, 12 (Jun 2019), 16861–16885. DOI: http://dx.doi.org/10.1007/s11042-018-7043-9

[142] Mythreya Seetharama, Volker Paelke, and Carsten Röcker. 2015. SafetyPIN: Secure PIN Entry Through Eye Tracking. In *Human Aspects of Information Security, Privacy, and Trust*, Theo Tryfonas and Ioannis Askoxylakis (Eds.). Springer International Publishing, Cham, 426–435. DOI: http://dx.doi.org/10.1007/978-3-319-20376-8_38

[143] Sherif Seha, Georgios Papangelakis, Dimitrios Hatzinakos, Ali Shahidi Zandi, and Felix JE Comeau. 2019. Improving Eye Movement Biometrics Using Remote Registration of Eye Blinking Patterns. In *2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2019)*. IEEE, USA, 2562–2566. DOI: http://dx.doi.org/10.1109/ICASSP.2019.8683757

[144] Reza Shadmehr and Thomas Brashers-Krug. 1997. Functional Stages in the Formation of Human Long-term Motor Memory. *Journal of Neuroscience* 17, 1 (1997), 409–419. DOI:http: //dx.doi.org/10.1523/JNEUROSCI.17-01-00409.1997

[145] Shaimaa Hameed Shaker, Eqbas Ali, and Israa Ahmed Abdullah. 2018. Security Systems Based On Eye Movement Tracking Methods. *Journal of Al-Qadisiyah for Computer Science and Mathematics* 10, 3 (2018), 70–78.

[146] Meng Shen, Zelin Liao, Liehuang Zhu, Rashid Mijumbi, Xiaojiang Du, and Jiankun Hu. 2018. IriTrack: Liveness Detection Using Irises Tracking for Preventing Face Spoofing Attacks. *CoRR* abs/1810.03323 (2018). http://arxiv.org/abs/1810.03323

[147] Daniel L. Silver and Adam J. Biggs. 2006. Keystroke and Eye-Tracking Biometrics for User Identification. In *Proceedings of International Conference on Artificial Intelligence (ICAI 2006)*. CSREA Press, USA, 344–348.

[148] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2016. Using Reflexive Eye Movements for Fast Challenge-Response Authentication. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 1056–1067. DOI: http://dx.doi.org/10.1145/2976749.2978311

[149] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2018. Analysis of Reflexive Eye Movements for Fast Replay-Resistant Biometric Authentication. *ACM Transactions on Privacy and Security* 22, 1, Article 4 (Nov 2018), 30 pages. DOI:http://dx.doi.org/10.1145/3281745

[150] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. EyeVeri: A Secure and Usable Approach for Smartphone User Authentication. In *IEEE International Conference on Computer Communication (INFOCOM'16)*. IEEE, USA, 1–9. DOI: http://dx.doi.org/10.1109/INFOCOM.2016.7524367

[151] Anugrah Srivastava. 2017. Biometric Identification System using Eye Movement Analysis. *International Journal of Engineering Science & Advanced Research* 3, 1 (2017), 77–83.

[152] Namrata Srivastava, Utkarsh Agrawal, Soumava Kumar Roy, and U. S. Tiwary. 2015. Human identification using Linear Multiclass SVM and Eye Movement biometrics. In *Eighth International Conference on Contemporary Computing (IC3 2015)*. IEEE, USA, 365–369. DOI: http://dx.doi.org/10.1109/IC3.2015.7346708

[153] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019a. Privacy-aware Eye Tracking Using Differential Privacy. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19)*. ACM, New York, NY, USA, Article 27, 9 pages. DOI: http://dx.doi.org/10.1145/3314111.3319915

[154] Julian Steil, Marion Koelle, Wilko Heuten, Susanne Boll, and Andreas Bulling. 2019b. PrivacEye: Privacy-preserving Head-mounted Eye Tracking Using Egocentric Scene Image and Eye Movement Features. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19)*. ACM, New York, NY, USA, Article 26, 10 pages. DOI: http://dx.doi.org/10.1145/3314111.3319913

[155] Nili Steinfeld. 2016. "I Agree to the Terms and Conditions": (How) do Users Read Privacy Policies Online? An Eye-tracking Experiment. *Computers in Human Behavior* 55 (2016), 992–1000. DOI: http://dx.doi.org/10.1016/j.chb.2015.09.038

[156] Yusuke Sugano, Xucong Zhang, and Andreas Bulling. 2016. AggreGaze: Collective Estimation of Audience Attention on Public Displays. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology (UIST '16)*. ACM, New York, NY, USA, 821–831. DOI: http://dx.doi.org/10.1145/2984511.2984536

[157] Abhishek Tiwari and Rajarshi Pal. 2018. Gaze-Based Graphical Password Using Webcam. In *Information Systems Security*, Vinod Ganapathy, Trent Jaeger, and R. K. Shyamasundar (Eds.). Springer International Publishing, Cham, 448–461. DOI: http://dx.doi.org/10.1007/978-3-030-05171-6_23

[158] Jayson Turner, Jason Alexander, Andreas Bulling, Dominik Schmidt, and Hans Gellersen. 2013a. Eye Pull, Eye Push: Moving Objects between Large Screens and Personal Devices with Gaze and Touch. In *Human-Computer Interaction – INTERACT 2013*, Paula Kotzé, Gary Marsden, Gitte Lindgaard, Janet Wesson, and Marco Winckler (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 170–186. DOI: http://dx.doi.org/10.1007/978-3-642-40480-1_11

[159] Jayson Turner, Andreas Bulling, Jason Alexander, and Hans Gellersen. 2013b. Eye Drop: An Interaction Concept for Gaze-supported Point-to-point Content Transfer. In *Proceedings of the 12th International Conference on Mobile and Ubiquitous Multimedia (MUM '13)*. ACM, New York, NY, USA, Article 37, 4 pages. DOI: http://dx.doi.org/10.1145/2541831.2541868

[160] Jayson Turner, Andreas Bulling, Jason Alexander, and Hans Gellersen. 2014. Cross-device Gaze-supported Point-to-point Content Transfer. In *Proceedings of the Symposium on Eye Tracking Research and Applications (ETRA '14)*. ACM, New York, NY, USA, 19–26. DOI: http://dx.doi.org/10.1145/2578153.2578155

[161] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3748–3760. DOI: http://dx.doi.org/10.1145/2858036.2858546

[162] Sarah Uzzaman and Steve Joordens. 2011. The Eyes Know What You Are Thinking: Eye Movements as an Objective Measure of Mind Wandering. *Consciousness and Cognition* 20, 4 (2011), 1882–1886. DOI: http://dx.doi.org/10.1016/j.concog.2011.09.010

[163] Filippo Vella, Ignazio Infantino, and Giuseppe Scardino. 2017. Person Identification through Entropy Oriented Mean Shift Clustering of Human Gaze Patterns. *Multimedia Tools and Applications* 76, 2 (Jan 2017), 2289–2313. DOI: http://dx.doi.org/10.1007/s11042-015-3153-9

[164] Mélodie Vidal, Andreas Bulling, and Hans Gellersen. 2013. Pursuits: Spontaneous Interaction with Displays Based on Smooth Pursuit Eye Movement and Moving Targets. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '13)*. ACM, New York, NY, USA, 439–448. DOI: http://dx.doi.org/10.1145/2493432.2493477

[165] Darius Vitonis and Dan Witzner Hansen. 2014. Person Identification Using Eye Movements and Post Saccadic Oscillations. In *Tenth International Conference on Signal-Image Technology and Internet-Based Systems*. IEEE, USA, 580–583. DOI: http://dx.doi.org/10.1109/SITIS.2014.116

[166] Volvo. 2019. Volvo Cars to Deploy In-car Cameras and Intervention Against Intoxication Distraction. https://www.media.volvocars.com/global/en-gb/media/pressreleases/250015/volvo-cars-to-deploy-in-car-cameras-and-intervention-against-intoxication-distraction. (2019). accessed 19 December 2019.

[167] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1403–1406. DOI: http://dx.doi.org/10.1145/2702123.2702212

[168] Justin Weaver, Kenrick Mock, and Bogdan Hoanca. 2011. Gaze-based Password Authentication through Automatic Clustering of Gaze Points. In *2011 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, USA, 2749–2754. DOI: http://dx.doi.org/10.1109/ICSMC.2011.6084072

[169] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Willy Wolff, Adam J. Aviv, and Zheng Wang. 2018. A Video-based Attack for Android Pattern Lock. *ACM Transactions on Privacy and Security* 21, 4, Article 19 (July 2018), 31 pages. DOI: http://dx.doi.org/10.1145/3230740

[170] Hong-Jun Yoon, Tandy R. Carmichael, and Georgia Tourassi. 2014. Gaze as a Biometric. In *Medical Imaging 2014: Image Perception, Observer Performance, and Technology Assessment*, Claudia R. Mello-Thoms and Matthew A. Kupinski (Eds.), Vol. 9037. International Society for Optics and Photonics, SPIE, USA, 39–45. DOI: http://dx.doi.org/10.1117/12.2044303

[171] Yanxia Zhang, Ming Ki Chong, Jörg Müller, Andreas Bulling, and Hans Gellersen. 2015. Eye Tracking for Public Displays in the Wild. *Personal and Ubiquitous Computing* 19, 5 (2015), 967–981. DOI: http://dx.doi.org/10.1007/s00779-015-0866-8

[172] Yongtuo Zhang, Wen Hu, Weitao Xu, Chun Tung Chou, and Jiankun Hu. 2018. Continuous Authentication Using Eye Movement Response of Implicit Visual Stimuli. *Proceedings of the ACM on*

Interactive, Mobile, Wearable and Ubiquitous Technologies 1, 4, Article 177 (Jan. 2018), 22 pages. DOI:http://dx.doi.org/10.1145/3161410

[173] Youming Zhang, Jorma Laurikkala, and Martti Juhola. 2014. Biometric Verification of a Subject with Eye Movements, with Special Reference to Temporal Variability in Saccades between a Subject's Measurements. *International Journal of Biometrics* 6, 1 (2014), 75. DOI: http://dx.doi.org/10.1504/ijbm.2014.059643

[174] Yun Zhang and Xuanqin Mou. 2015. Survey on Eye Movement Based Authentication Systems. In *Computer Vision*, Honbin Zha, Xilin Chen, Liang Wang, and Qiguang Miao (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 144–159. DOI: http://dx.doi.org/10.1007/978-3-662-48558-3_15

[175] Youming Zhang, Jyrki Rasku, and Martti Juhola. 2012. Biometric Verification of Subjects Using Saccade Eye Movements. *International Journal of Biometrics* 4, 4 (Oct. 2012), 317–337. DOI: http://dx.doi.org/10.1504/IJBM.2012.049736

[176] Huiyuan Zhou, Vinicius Ferreira, Thamara Alves, Kirstie Hawkey, and Derek Reilly. 2015. Somebody Is Peeking!: A Proximity and Privacy Aware Tablet Interface. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. ACM, New York, NY, USA, 1971–1976. DOI: http://dx.doi.org/10.1145/2702613.2732726

[177] Huiyuan Zhou, Khalid Tearo, Aniruddha Waje, Elham Alghamdi, Thamara Alves, Vinicius Ferreira, Kirstie Hawkey, and Derek Reilly. 2016. Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1362–1373. DOI:http://dx.doi.org/10.1145/2858036.2858232